PNP Computer Security Bulletin CSB18-02

Meltdown and Spectre Vulnerabilities

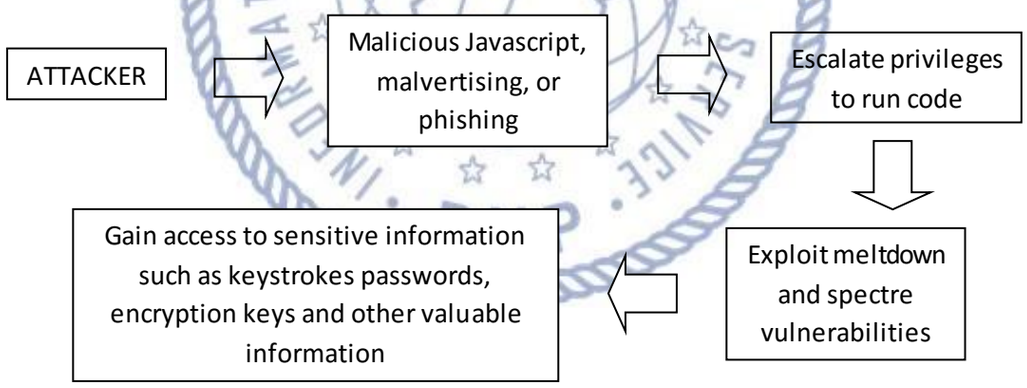
Risk/Impact Rating: **SERIOUS**

Created: January 29, 2018

Description:

- CPU hardware implementations are vulnerable to side-channel attacks
- Meltdown is a bug that "melts" the security boundaries normally enforced by the hardware, which affects desktops, laptops, and cloud computers
- Spectre is a flaw that an attacker can exploit to force a program to reveal its data, which affects almost all devices including desktops, laptops, cloud servers, and smartphones
- Meltdown is easier to exploit because the program to steal passwords and other data can be hidden on a website, while Spectre requires more direct access to the microchip, but affects CPU, and is not easily patched; however this is more difficult to exploit
- It's a speculative execution which is an optimization method a computer system performs to check whether it will work to prevent a delay when actually executed
- The vulnerabilities can allow passwords and other sensitive data on chips to be read.

How it works:



Modus Operandi:

- Malicious Javascript, malvertising, or phishing hidden on a website.

Solution:

- NCCIC encourages users and administrators to refer to their hardware and software vendors for the most recent information.
- Firmware update and patches released by manufacturers.

Intel:

Intel has posted a security alert regarding microcode updates related to Variant 2 of Spectre (CVE-2017-5715). More information can be found here: https://newsroom.intel.com/news/root-cause-of-reboot-issue-identified-updated-guidance-for-customers-and-partners

Additionally, Intel has provided “Microsoft Revision Guidance”, which lists a variety of Intel products and associated guidance for patching. It is found here in PDF format: https://newsroom.intel.com/wp-content/uploads/sites/11/2018/01/microcode-update-guidance.pdf

Microsoft:

Microsoft, which had temporarily halted updates for AMD machines, has provided updated patches. More information can be found here: https://support.microsoft.com/en-us/help/4073707/windows-operating-system-security-update-for-amd-based-devices

For machines running Windows Server, a number of registry changes must be completed in addition to installation of the patches. A list of registry changes can be found here: https://support.microsoft.com/en-us/help/4072698/windows-server-guidance-to-protect-against-the-speculative-execution(link is external).

Security Risks to PNP Computer Systems and Data:

- Sensitive information could be revealed from a computer’s kernel memory, which could contain keystrokes, passwords, encryption keys, and other valuable information.
- Interfere with the normal functioning of the computer system or prevent its utilization.

Mitigation Measures:

- Update system regularly;
- Lookout for any and all future security releases and install them immediately;
- Back up and test your data regularly;
- Avoid opening e-mails from unverified or questionable sources;
- Avoid illegal websites or torrent sites;
- Use genuine software and patch/update;
- Scan your computer regularly using antivirus software;
- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching the end users; and
- Run regular penetration tests as often as possible and practical.

If infected:

- Download any and all software patches or microcode.

References:

- https://www.reuters.com/article/us-cyber-security-microchips-explainer/explainer-how-chip-flaws-spectre-meltdown-work-and-whats-next-idUSKBN1F102X
- https://www.us-cert.gov/ncas/alerts/TA18-004A
- https://spectreattack.com/spectre.pdf

For further inquiries, contact ITMS ISSD:

- Telephone Number: **(02) 723-0401 local 4225**;
- E-mail address: **issditms@gmail.com**; and
- Chat Service: **www.itms.pnp.gov.ph**.